Analysing Information Security in a Bank using Soft Systems Methodology

Abstract

Purpose –This paper explores the use of Soft Systems Methodology (SSM) to analyse the socio-technical information security issues in a major bank.

Design/methodology/approach – Case study research was conducted on a major bank. Semi-structured interviews with a purposive sample of key stakeholders in the business, comprising senior managers, security professionals and branch employees were conducted.

Findings – SSM was particularly useful for exploring the holistic information security issues, enabling models to be constructed which were valuable analytical tools and easily understood by stakeholders, which increased the receptiveness of the bank, and assisted with member validation. Significant risks were apparent from internal sources with weaknesses in aspects of governance and security culture.

Research limitations/implications – This research uses a single case study and whilst it cannot be generalised, it identifies potential security issues others may face and solutions they may apply.

Practical implications - Information security is complex and addresses technical, governance, management and cultural risks. Banking attacks are changing, with greater focus on employees and customers. A systemic approach is required for full consideration. SSM is a suitable approach for such analysis within large organisations.

Originality/value – Demonstrates how important benefits can be obtained by using SSM alongside traditional risk assessment approaches to identify holistic security issues. A holistic approach is particularly important given the increasing complexity of the security threat surface. Banking was selected as a case study since it is both critical to society and is a prime target for attack. Furthermore, developing economies are under-represented in information security research, this paper adds to the evidence base. Since global finance is highly interconnected, it is important that banks in such economies do not comprise a weak link and hence results from this case have value for the industry as a whole.

Key words: Information Security Management System (ISMS), Soft Systems Methodology (SSM), Socio-technical Risks, Banking Security, Security Governance, Information Security Culture.

Paper Type – Case study/ Research paper

1. Introduction

Modern economies are highly reliant on the banking industry, a fact that is amply demonstrated by the 2008 world-wide financial crash, so the importance of maintaining effective information security in banks is critical. Indeed, Raytheon (2015) concludes that a cyber-crisis at one or more banks could result in financial catastrophe, not only to customers and banks, but to a country's financial system as a whole.

Consequently, a bank which fails to protect its information systems not only loses its competitive advantage, but also threatens its existence (Von Solms, Thomson and Maninjwa, 2011). Ultimately, the success of a bank can depend on its ability to manage its information security and provide secure services (Ula, Ismail & Sidek, 2011) and it is hardly surprising, therefore, that 80 percent of leaders in the financial services sector cite cyber risks as a top concern (Travelers, 2015).

Moreover, the threats that banks face are amplified by customers' expectations. Customers want to interact easily, yet securely with their bank in real time through an increasing range of mobile services. The expansion of these services increases the attack surface and consequent security threats, the number and complexity of attacks and the resultant losses are increasing rapidly. In 2012, between £48m and £1.5bn was stolen from thousands of bank accounts across Europe, the US and Latin America (Wilson, 2013). In 2015, Kaspersky revealed cyber-attackers targeted up to 100 banks, e-payment systems and other financial institutions in around 30 countries stealing $1bn within two years. A sophisticated cyber-attack on JPMorgan Chase & Co compromised information of 76 million households and 7 million small businesses (Weise, 2014). Banks (and their customers) are a prime target for cyber-criminals, one UK bank reports over 1000 attacks per day[i] and most significantly, Raytheon (2015) reports that financial services companies encounter security incidents 300% more frequently than other industries.

It is, therefore, essential to understand the risks in this industry, and implement effective controls. The ISO27000 series of International Standards represent current 'best practice' for defining, auditing and managing an ISMS in a systematic way. It relies on a top-down approach, identifying assets, risks to those assets and suitable controls. Whilst this mechanistic approach can certainly be effective, its focus on system *components* raises the possibility of omitting *systemic* risks, particularly those that span governance, management, and cultural aspects of information security.

The Symantec report (2012) acknowledges that the financial industry has a superior level of technical controls but emphasizes that any effective treatment of risks must take an holistic (systems) approach,

since an increasing number of attacks are aimed at people – both employees and customers. Unfortunately, most research has focussed on technology and more work is required on the socio-technical aspects of information security (Hagen, Albrechtsen, & Hovden, 2008)

In response to this need to focus on the socio-technical threats, and Karlsson *et al's* (2015) exhortation for more empirical and in-depth research, this paper presents a case study of a major bank in a developing economy. Since global finance is highly interconnected, it is important that banks in such economies do not comprise a weak link and hence results from this case have value for the industry as a whole.

Therefore, this study analyses the current state of the bank's Information Security Management System (ISMS) and explores how well the current culture supports it. It provides an important contribution as it addresses a critical, under-researched and growing concerns for information security within the banking industry, examining how it is being addressed within a major bank within a developing nation, and identifies lessons that can be learned together with a model that can be applied beyond this particular organization.

The research questions explored were:

1. How effective was SSM for assessing holistic socio-technical information security risks in a complex organisation?
2. What is the current status of the ISMS practices in the bank?
3. What are the information security challenges and risks facing the bank and in particular the socio-technical risks?
4. How can the bank improve its ISMS?

A further key feature of this research is that it evaluates the use of Checkland's (1999) Soft Systems Methodology (SSM) as the analytical framework. Checkland's methodology is particularly useful to capture the systemic complexities within an organisation. Thus, it appeared to be a useful approach for assisting organisations to improve security governance and management practices. By bracketing the technological risks, the SSM approach focuses upon the emergent and systemic socio-technical risks present in modern banking.

This paper is organized as follows. Section two's evaluation of the literature on ISMS reveals the inadequacy of research into cyber security in general, and an acute shortage of knowledge on developing countries' ISMS. Section three explains how SSM is used as a framework for the research. Section four presents the data analysis and identifies actions required to improve the ISMS

of the bank together with a model. Section five concludes the paper and provides recommendations which have wider applicability.

2. Literature Review

This research focuses on socio-technical information security risks in the banking industry. Tarimo, (2006) explained that socio-technical systems are characterised by complex systems, i.e. systems which have complex behaviours (such as non-predictability and emergence) and contain parts interacting in a non-linear fashion. Analysing the security of these socio-technical systems require reviewing the aspects which can harm as well as protect them. It is therefore important to analyse the changing socio-technical threat landscape for the banking industry. These show a trend to target the human element of the system. Consequently, the review explores how these socio-technical threats are controlled, highlighting the importance of (and weaknesses in) governance, management and culture.

The Changing Nature of Security Threats

The threats facing the banking sector are evolving rapidly; just five years ago cyber-attacks were not recognised as a primary threat but just one of many. In 2011, Ula, Ismail, & Sidek identified the following threats: physical destruction of premises and systems by natural disasters; unintentional damage due to human error; abuse of system and sensitive information by employees or agents of the bank; systematic collection of sensitive information by foreign intelligence services; and external attacks which compromise confidentiality, integrity and availability of information.

Whilst this list could apply to most large industries, it is more significant that the financial sector was one of the first to be targeted by industry-specific cyber-attack techniques. The potentially high rewards available from compromised banking systems have meant that criminals spend an enormous amount of time on reconnaissance and in crafting convincing lures to trick employees and customers into installing malware or visiting spoof sites (Raytheon/Websense, 2015).

This trend to target employees has been increasing with the most common subjects of phishing emails being of professional nature (e.g. *Bacs* Payment Schemes, for payments, invoices). Alongside this, cybercriminals bombard sites with low-level attacks (e.g. low-level Distributed Denial of Service attacks (DDOS)) to provide background noise which distracts security staff from targeted attacks (Raytheon/Websense, 2015). Thus, we are seeing what Symantec (2012) calls ‘refined social

engineering' as a focus of attack. Furthermore, the increased use of social media by employees at work provides yet more opportunity for the attackers.

These social engineering attacks that target employees supplement the threat already posed by direct attacks on bank customers in order to capture personal authentication details. Major attack methods that are used include phishing, typosquatting (un-noticed miss-spelled URLs) and black-hat Search Engine Optimisation techniques to raise chance of victims visiting spoof bank websites. (Raytheon/Websense, 2015). Online banking fraud increased from £40.9m to £60.4m in the UK in 2014, a 48% rise and another major contributor was the recent increase in Telephone-based deception crimes (FFA, 2015).

External security risks have received considerable attention in the banking industry. However, insider attacks are yet another threat which is exhibiting increasing severity, frequency, and complexity. A security breach at Société Générale resulted from malicious behaviour by an employee incurring a cost of $7 billion (Udeh & Dhillon, 2008). While financial gain is the main motivation for insider attacks, discontented employees are also a threat (Mulwa, 2012). It is also worth noting that employee mistakes and accidents are often causes of incidents (Lacey, 2009).

A clear trend is has therefore emerged and whilst technology can be helpful in reducing risks (e.g. email filtering), the real target (or vulnerability) in these cases is the human, so it is essential that security controls address the human element of organisations. Hagen, Albrechtsen, & Hovden 's (2008) survey in Norway found that the most common such control (84% of organisations) was a security policy, signifying a governance-led response.

Information Security Governance (ISG) in Banks.

Information Security Governance (ISG) integrates information security into an organisation's overall corporate governance responsibilities (Posthumus and von Solms, 2004). Dealing with risks associated with information security like any other business risk is considered good practice (Symantec, 2012). Effective ISG is fundamental for establishing information security in banks and, therefore, to achieve their business objectives. Various ISG frameworks have been developed to establish organizational information security (Da Veiga and Eloff, 2007).

ISG is a responsibility of the senior management of the organisation. ISO27001:2013 mandates that the executive management should produce a Corporate Information Security Policy (CISP) to direct information security. The CISP is strategic level interpretation and expression of the directives which form a basis for all tactical and operational level policies. Consequently it is one of the most

important documents in applying information security governance and it must be created with due care (Von Solms, Thomson and Maninjwa, 2011; Hone and Eloff, 2002). However, the lack of proper ISG is a significant cause for security breaches in the banking sector, exemplified by the root cause of the previously mentioned breach at Société Générale. Furthermore, it is also evident in different sectors of developing countries, including banking. Tarimo's (2006) study on socio-technical aspects of Tanzanian organizations' ICT security revealed that there was no defined security goals and ICT security policy in the organizations studied as well as at the national level. Thus, ISG practices should constitute a focal point for risk assessment.

Tsiakis, *et.al* (2014) explored whether an IT security governance (ITSG) program can mitigate e-banking risks. They evaluated ISG frameworks, international standards, 'best practices', principles, and risk management methods against standard ISG objectives. An important finding was that each ITSG approach has its own benefits and shortcomings and no single approach is 'best fit' for e-banking. The adoption of a particular ITSG approach in banking depends on the size, financial strength, culture, core competencies and overall security strategy the bank employs in accordance with the business objectives.

This point of organisational fit is critical, it is a common pitfall to develop information security strategies, policies, processes and procedures and try to enforce them without understanding how organisational culture impacts their effectiveness (Hamidovic, 2011). Effective security cannot be created by directing and controlling alone. It needs a supportive security culture (ISACA, 2011). Unfortunately, it is often overlooked. For example, a study of five Pakistani banks revealed that properly implemented technical and operational security controls existed but information security culture was missed (Munir & Manarvi, 2010). Similarly, staff in 58% of Nigerian banks lack knowledge of their bank's information use policies which are fundamental to create information security culture (Mulwa, 2012). A study on 8 commercial banks that offer e-banking services in Zimbabwe revealed that most of the times they failed to meet behavioural security requirements although the other elements of information security are adhered (Ngwenya and Malufu, 2012).

Both governance and management are essential to control security risks (Posthumus & von Solms, 2004). The next section therefore moves on to examine information security management.

Information Security Management in Banks

Information security risk management is the main component of an ISMS and should be seen as a component of corporate risk management. The banking industry uses Basel III to manage corporate

operational risks, which directly relate to information security risk management (Locher, 2005). Munir & Manarvi (2010) argue that information security management should be combined with operational risk management.

Information security standards, frameworks and models, such as ISO 27001, PCI DSS, COBIT 5 and BMIS (ISACA, 2011), have an influential impact in improving information security management of the banking industry. They help attain adequate level of security although they cannot guarantee 100% security (Susanto *et al*., 2011). There is no standard, framework or model which can address all security concerns and 'best fit' for all organisations including banks. For example, Zuccato (2006:257) criticises ISO27001 that it is not entirely suitable for e-commerce, as it is tailored for a "conventional" organization, and its risk analysis approach alone is not sufficient to derive the security requirements in e-commerce. This is another critical point - once again it reinforces the important message that a rigid approach is likely to leave gaps in addressing socio-technical aspects of information security, and this research therefore addresses the gap by exploring how the SSM (based on the individual organisation's requirements) can address this weakness.

Information Security Culture

Whilst information security governance, management and the use of associated tools are important, a common theme runs through all the literature: that of a complex socio-technical system and the need to establish an 'Information Security Culture'. Karlsson *et al's* (2015:247) systematic review summarised the consensus definition as 'A shared pattern of values, mental models and activities that are traded among an organisation's employees over time, affecting information security'. The definition immediately throws up problems, particularly in large organisations, for example: how can you achieve shared values? Large organisations have many departments, staffed by people of varied expertise, backgrounds and, importantly, different goals. In addition, the organization may have branches located in different countries with different national cultures which can affect the security culture of the organisation's branch in each jurisdiction. Chaula's (2006) socio-technical analysis on information security of a Tanzanian company identified that national cultural dimensions *(i.e. uncertainty avoidance, future orientation, assertive orientation, power distance and gender egalitarianism)* have implications for organizational security. In short there will be sub-cultures in any large organisation, and value conflicts are certain to arise, particularly with information security, which is often seen as a barrier to the business, rather than an enabler. Hedstrom *et al*., (2011)

considers the control-based compliance model, which is implicit in the governance and management approaches outlined above, as a contributor to the conflict.

Calls to improve security awareness are common (e.g., Thomson & von Solms, 1998; Siponen, 2000; OECD, 2015). For example, HDFC Bank in India promoted security culture by displaying the user policy document in summarized ten security commandments, developed from the behaviours identified in COBIT 5 (Salvi, 2013). Zuccato (2006) proposed a holistic security management framework which incorporates human and organization workflow to address security awareness and related concerns.

The organisational culture is formed over time by strategy, organisational design and people's behaviours at work. Consequently, awareness alone is insufficient to create a positive security culture (one where each member is helping each other to do the right thing) (ISACA, 2011). According to ISACA (2010), the most effective changes in the perception of information security tend to happen when a board level senior manager assumes responsibility for security and reshapes the organisational culture and Chaula (2006) emphasizes management commitment to security is essential for successful development of an organizational security culture.

On a study regarding the effect of information security culture in Nigerian Banking, Selamat and Babatunde (2014) identified five variables which are related to the development of information security culture that will improve organizational performance: information technology; international security standards; perceived information security risk, threat and vulnerabilities; motivation of employee; and perceived job roles and responsibilities. Interestingly, this list has a predominantly technical bias, whereas other authors highlight the managerial practices to change attitudes and behaviours. Hagen's (2008) survey shows that awareness creation (campaigns, user training, user participation, top management engagement) had the greatest impact on security - emphasizing the significance of culture in maintaining good security and Chaula (2006) provides further detail, suggesting eleven security dimensions to create a security culture: management commitment, awareness orientation, people orientation, risk orientation, information classification, assurance orientation, future orientation, uncertainty avoidance, standards adoption and compliance, attention to details and ethical orientation.

Organisational culture is both complex and dynamic, to develop a security culture needs a method of assessing it. Tarimo (2006) presented a checklist to assess the socio-technical ICT security readiness of developing countries. The checklist covers ethical/cultural, legal/contractual, administrative/managerial, operational/procedural, and mechanical/electronic controls. Okere, Van

Niekerk and Carroll (2012) used Schein's (2009) 3-level model of organizational culture as a basis for analysing information security culture assessment approaches and they concluded that whilst current approaches utilize some form of auditing as an assessment method, none have followed a formal auditing approach utilizing an established audit framework.

The concept of such a framework is attractive when dealing with complex situations like information security, and Da Veiga and Eloff (2010:197) describe an "all-encompassing framework for cultivating and ultimately assessing culture". It comprises a 3-layer model of components (artefacts such as policy) which influence behaviour, and in turn promotes culture. Whilst there is a feedback loop from culture to component, the predominant direction is that culture is produced mostly from components in a quite *directive* and deterministic way and it hardly acknowledges the messy detail of shared tacit assumptions.

Summary: Analysing Socio-technical Aspects of Security

This brief review has established key points that are relevant to this research. Firstly, there is a consensus that banks are a prime target for attack and there is a significant increase in the targeting of the human element of the system (employees as well as customers), often through 'refined social engineering' techniques.

Secondly, the review establishes that technical solutions alone cannot control the associated risks. Consequently, researchers recommend deployment of a holistic approach to ensure 'security in depth'. The key aspects involve governance, commitment from senior management, deployment of management tools, and programmes to create a security culture.This review also revealed that current methods of promoting and assessing security culture have significant weaknesses, including that they use questionnaires to assess culture. Questionnaires do not reveal the interaction and patterning in the cultures and subcultures and only assess superficial characteristics of the culture because survey instruments cannot get at the deeper shared tacit assumptions that define the essence of cultures (Schein, 2009). Lacey (2009) recommends addressing this weakness by emphasizing genuine *engagement with employees* rather than infrastructure & formal procedures.

It is therefore clear that there is a need for research which focuses on the assessment of socio-technical aspects of security which are of increasing importance. Moreover, prevalent approaches to security assessments have typically followed mechanistic approaches, focussing on *components* and therefore possibly omitting *holistic* issues. Lastly, since organisational culture has been shown to be critical, an approach that engages employees is needed. To capture these aspects, a systemic approach

is needed and therefore this research evaluated Soft Systems Methodology. SSM is a 'reaction to the inadequacy of so-called 'hard system' approaches in solving problems that involved a component of human activity' (Reviewer1, 200x:x).

Checkland's (1999) Soft Systems Methodology appears very attractive in this context: it is designed as a problem-solving methodology for complex and messy situations, creating a variety of models to represent the situation(s). SSM is an action-oriented problem solving methodology which facilitate taking action to bring a change (Reviewer1, 200x). Importantly, SSM is suitable not only to conduct the socio-technical security analysis but also to engage stakeholders and identify potential *culturally feasible* solutions therefore acknowledging and influencing organisational culture (and organisational differences). It is discussed in the next section.

3. Methodology

Karlsson *et al's* (2015) systematic review of information security culture research identifies that almost 40 percent of the papers are theoretical and do not include empirical data. Unlike those papers, this research is based on empirical data and it is conducted with a qualitative interpretivist approach using an embedded single case study methodology. A Case Study has a particular strength of collecting detail and providing an in-depth illumination of the specific context (Yin, 2009). In addition, it helps to uncover the day to day information security practice of the bank rather than specified procedures and policies. The case is of particular interest since it is amongst the biggest banks within the country with a nationwide network of branches and a core banking system providing internet and mobile banking services.

The research received ethical clearance from the university and paid particular attention to protecting the human subjects ensuring informed consent, anonymity, secure data storage and privacy. Any concerns of the bank were discussed and resolved during the project.

Semi-structured interviews were used to collect data, since they enable an outline agenda to be followed whilst maintaining the flexibility to explore responses in more detail (Alfawaz, 2011). A purposive sample was used, selecting staff with roles most relevant to the research from senior business management, security professionals and branch employees. Fifteen interviews were conducted. Ten involved a role directly related to information security, five were with staff in the bank's branches. Interviewees were: Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Project Management Officer (CPMO), Electronic Banking Director (EBD), Application & Infrastructure Director (AID), Risk Manager, Infrastructure Manager, Security

Operation Manager, Security Audit Manager and Security Management Officer. The remaining five interviewees were: Branch Manager, Customer Service Manager, Customer Service Officer, Controller and Cashier.

The sample size taken to explore the overall information security management and governance situation can be considered as representative. However, the sample of employees taken to identify the information security awareness and culture in the bank was small relative to the total number of bank employees. Despite this limitation, all the interviewees including the senior managers, managers, security professionals and selected employees provided consistent replies regarding the state of information security awareness and culture. This consistency increases the confidence that the sample size limitation will not have considerable impact on the conclusion regarding security awareness and culture.

Data were analysed using Soft System Methodology (SSM) which Checkland & Poulter (2006: 22) describe as an 'action oriented process of inquiry into problematic situations'. The theoretical lens of SSM is used to capture the unstructured and systemic complexities within a human activity system.

SSM involves seven stages which lead to five different actions. The four main actions, followed in the analysis, are shown below. The fifth action is iterating the primary four, namely critical reflection on the whole process (Checkland and Poulter, 2006).

1. Exploring & expressing the situation in which the problem lies through structure and process, using a 'Rich Picture' and system 'root definition'.
2. Building purposeful models judged to be relevant to the situation.
3. Using the model to question the real world. This brings structure to a discussion about the situation which aims to find changes which are both arguably desirable and also culturally feasible in this particular situation.
4. Define/take the action to improve the situation.

4. Analysis and Discussion

The section explains how SSM was applied to analyse the information security management practices of the bank. Results are presented primarily through the artefacts of SSM, together with supporting text.

Exploring the Current Problematic Situation

SSM starts by exploring the problem situation, rather than working from a well-defined problem. This approach reduces assumptions and the likelihood of omitting relevant information. A 'Rich Picture' is constructed to represent the situation.

A Rich Picture helps to encourage holistic rather than reductionist thinking about the situation. It captures informally, the main entities, structures and viewpoints in the situation, the processes going on, the current recognized issues and any potential ones as a basis for discussion (Checkland and Poulter, 2006).

A Rich Picture (Figure 1) was used to represent the system through the views of interviewees, who were representatives of the main internal and external stakeholders. This diagram captures the interview results in a way that is much more succinct than traditional participant quotes, and graphically shows relationships. This section discusses key points arising from the Rich Picture.

The CIO explained that the bank's mission includes implementing state-of-the-art technology, and information security is the central part of IT and one of the focus areas of the bank's strategy. Projects are initiated to implement the strategy. *Although the currently running project considers improving the information security governance and awareness, the CIO views information security dominantly from an IT perspective.* The CPMO also explained that security issues are mentioned in the IT strategy although there is no separate information security strategy and it is expected to be proposed by the security department.

All interviewees agreed that the information security management system of the bank was not mature even though the bank is working on a security project to create a foundation for its improvement. The CPMO noted that currently there is no information security management system and the information security is managed in an unsystematic way although technical security controls are placed properly. He emphasized that the security department was not efficiently addressing the required information security tasks, and recruiting professionals is a major challenge. In contrast, the Security Management Officer mentioned lack of security training as one factor for not efficiently addressing the required information security tasks.

The bank faces considerable internal and external risks. The Infrastructure Manager and the CISO explained that they have identified attack trails originating from different countries. However, they considered that most of the risks and challenges are internal, and were the main concerns as emphasized by the CPMO:

"My main worry is on the internal risks. I don't worry much on internet and mobile banking risks".

The Infrastructure Manager elaborated these risks as internal threats which he considered were caused mainly by non-technical shortcomings. He listed these as a lack of: segregation of duties, security awareness, ISMS framework, security policy, procedures and guidelines, and skilled professionals. Password sharing is also common. The Security Management Officer emphasized that the lack of security policies and procedures makes it difficult to enforce security controls and develop security culture.

In addition to the lack of security awareness, a further critical factor that the Branch Manager identified was that employees do not have an adequate focus on information security since security is not considered in their performance evaluation. The lack of synergy between departments and improper attitude towards security and security audit is also another challenge. The EBD explained:

"In the past, we were taking security as extra task which hindered our operation and we used to consider security auditors as fault finders and accusers, and we had no collaboration with them. Currently we have a good attitude towards security and security auditors, and we proactively request them to audit our systems".

The improvements in this regard are due to the increasing security awareness of the senior management and the Electronic Banking Department. However, the EBD noted that the business and the security are not efficiently integrated and this has caused challenges for both the business and security. Therefore, she emphasized that:

"The security solutions should be customer centric and customer friendly. The security shouldn't be as expense of the service. Our internal compromises are due to our customer centric view".

It is worth emphasizing here that these are not typically risks that would be identified by traditional ISO27001/ISO27005 assessments.

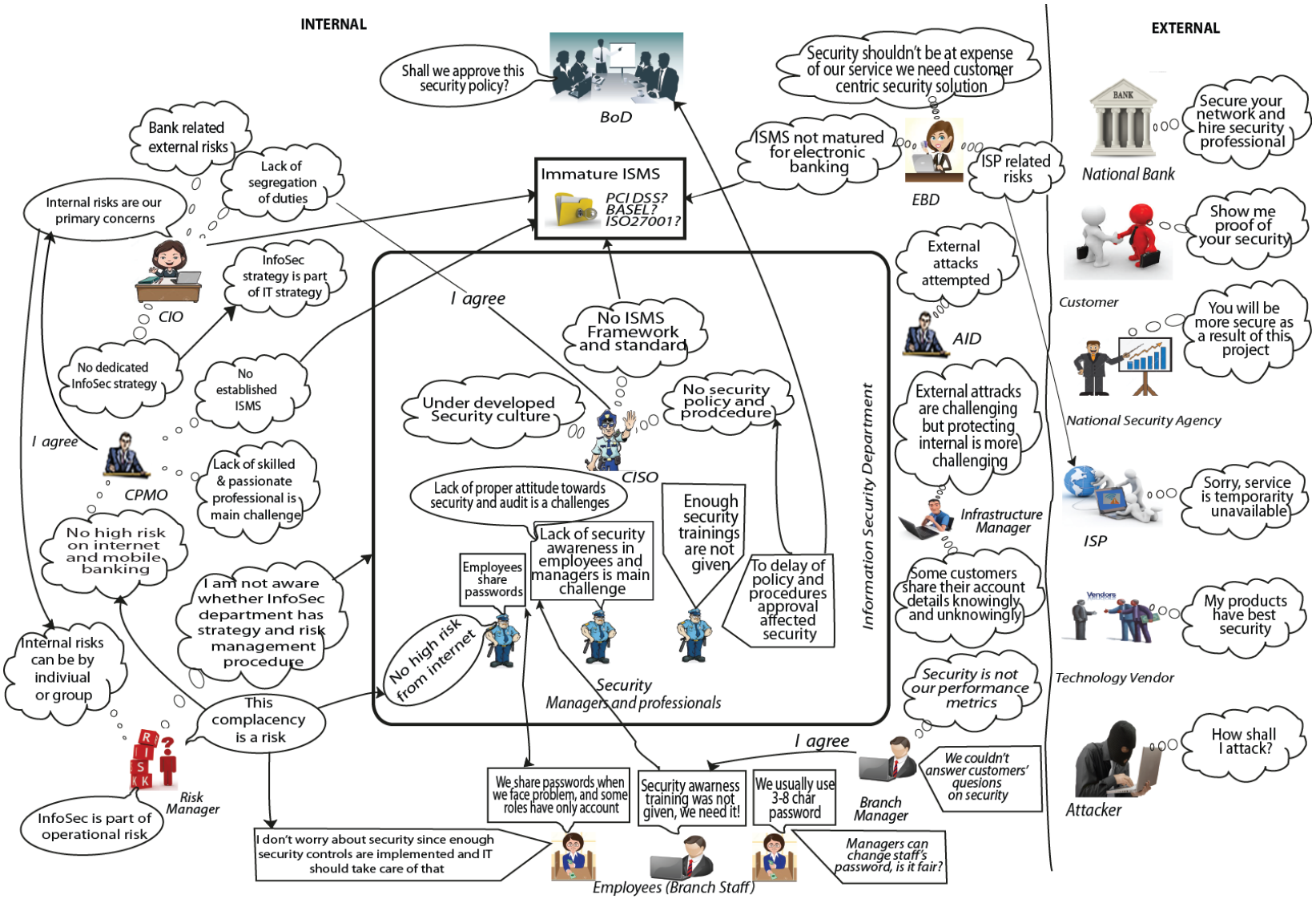

Figure 1: Rich picture of the bank's information security situation[ii]

The CISO said he felt that the IT professionals lack cooperativeness and they sometimes compromise security to avail the service. On the other hand, the Infrastructure Manager argued that the IT Operation Department was jointly working with Security Department, follows good practices and doesn't compromise security for the sake of availability/operation.

Table 1 summarizes the main risks and challenges that are emphasized by the interviewees and those who have mentioned them.

Table 1: The main risks and challenges of the bank

Main challenges and vulnerabilities	Category (Theme)[1]	CIO	CPMO	CISO	EBD	AID	Infrastructure Manager	Security Operation Manager	Security Audit Manager	Security Management Officer	Risk Manager	Branch Manager	Customer Service Manager	Customer Service Officer	Controller	Chief Cashier
Immature ISMS	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					
Lack of security awareness	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password sharing	2	✓		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Limited professional capacity	4	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓				
Lack of security policy and procedures	1		✓	✓	✓			✓	✓	✓					✓	
Lack of InfoSec[2] performance evaluation	1		✓	✓								✓				

[1] The category (theme) number shows the category of the main challenges and vulnerabilities on the concept map shown in Figure 2 below

[2] InfoSec stands for Information Security

Concept Map of the Situation

In addition to the rich picture, the overall information security situation is summarized using the concept map (Figure 2) shown below, helping to express the analyst's view of entire information security situation in organized way.

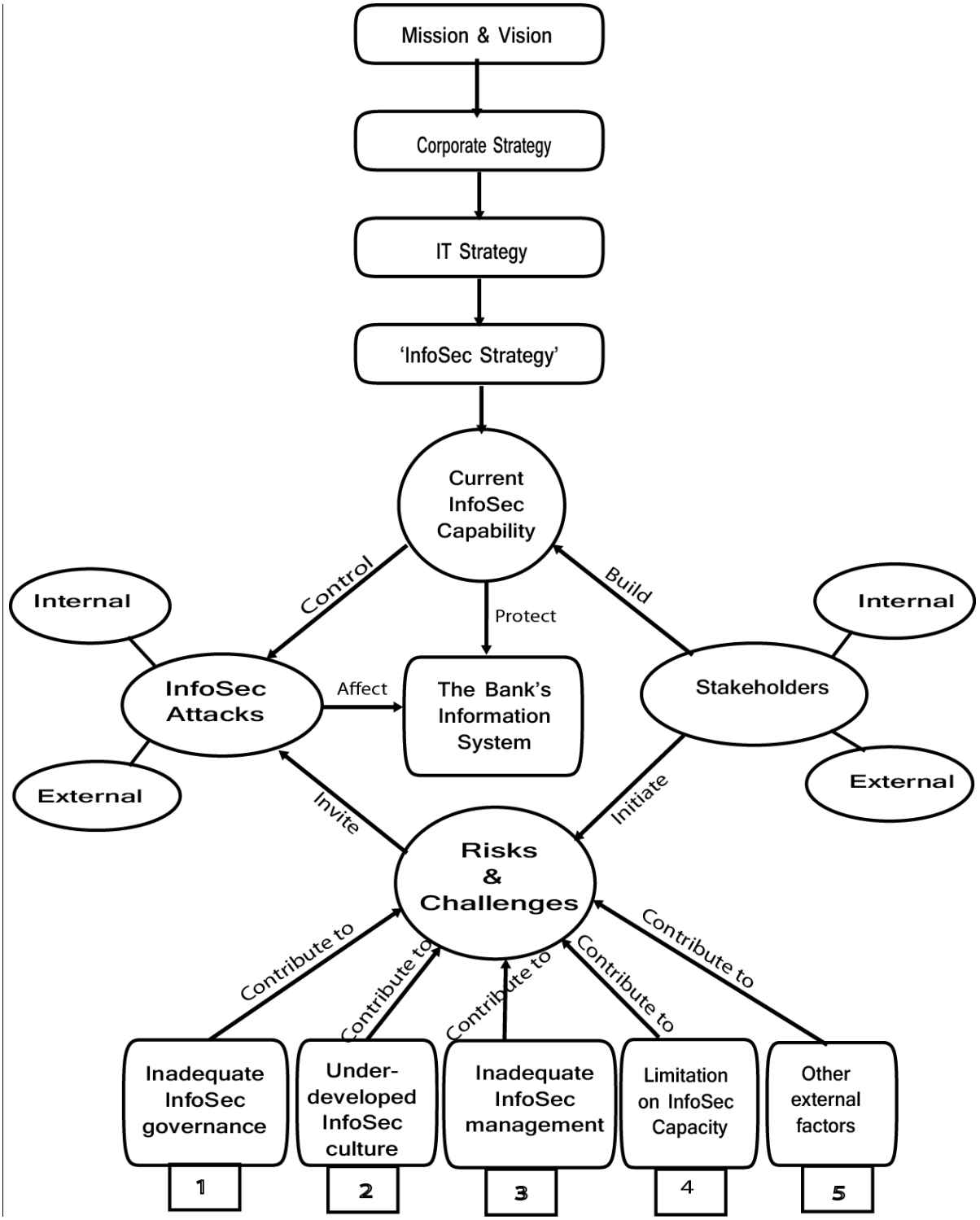

Figure 2: Concept map of the bank's information security situation

The above concept map shows the *current* information security situation of the bank with emphasis on security risks and challenges. The following section develops a further model which will help to address this problematic situation and improve the information security of the bank.

Developing further Models

SSM requires a statement, called Root Definition (RD), which describes the activity system to be modelled as a transformation process. The RD is written as a statement based on the output of the 'PQR formula'. The PQR formula involves '*do P by Q in order to help achieve R'*, where PQR answer the questions: 'What?' 'How?' and 'Why?' respectively (Checkland and Poulter, 2006).

The root definition adopted by the analysts is:

A bank-owned and operated system (ISMS), staffed with skilled professionals with the right attitude, to secure the bank's information system by means of suitable information security controls, derived from information security good practices (standards, frameworks and models), in order to provide efficient and effective risk-based information security which best realize stakeholders' needs and support national development.

The root definition involves six elements of the situation as a system: Customers, Actors, Transformation, Waltanschauung (world-view), Owners and Environment which are known by the mnemonic 'CATWOE'. These elements of the bank are described as follows.

Customers are those who benefit from the bank's ISMS. *Customers* include the bank's customers, government and the bank's stakeholders. *Actors* are people who transform inputs into outputs. The main Actor is the Security Department of the bank. Addition Actors include Risk Management, IT Audit, Information Systems, E-banking and Project Management Divisions. The *Transformation* is from an ineffective ISMS to a mature effective ISMS. The *Waltanschauung* is the broader context and worldviews. The worldview adopted here is 'the information security of the bank can be improved by using effective ISMS'. The *Owners* of the problem are the bank's Board of Directors and Security Department. The *Environment* constraints include: lack of security awareness and under-developed security culture in the public; lack of security companies and training institutes in the country; and shortage of security professionals in the country.

In addition to the CATWOE elements, SSM requires identification of the measures of performance by which the operation of the system will be judged (Checkland and Poulter, 2006). The three relevant criteria are:

1. **Efficacy (E1)**: criteria to tell whether it is producing its intended outcome.
2. **Efficiency (E2)**: criteria to tell whether it is being achieved with a minimum use of resources.
3. **Effectiveness (E3)**: criteria to tell whether it is helping to achieve some higher-level or long term aim.

The criteria to measure the performance of the bank's ISMS are:

1. **E1**: Are the suitable information security management controls in place? Is the ISMS practiced (established, implemented, operated, monitored, audited, reviewed, maintained and improved) in compliance with applicable standards?
2. **E2**: Is the ISMS (and the security management controls) worth the resources consumed? Is the return on security investment (ROSI) acceptable?
3. **E3**: Is the bank's information system secure? Does security enable the bank to achieve its business objectives with minimum risk (to best realize stakeholders' needs and support national development)?

Based on the RD, CATWOE and E1, E2, E3 mentioned above, the conceptual activity model of the bank's ISMS (Figure 3) is shown below.

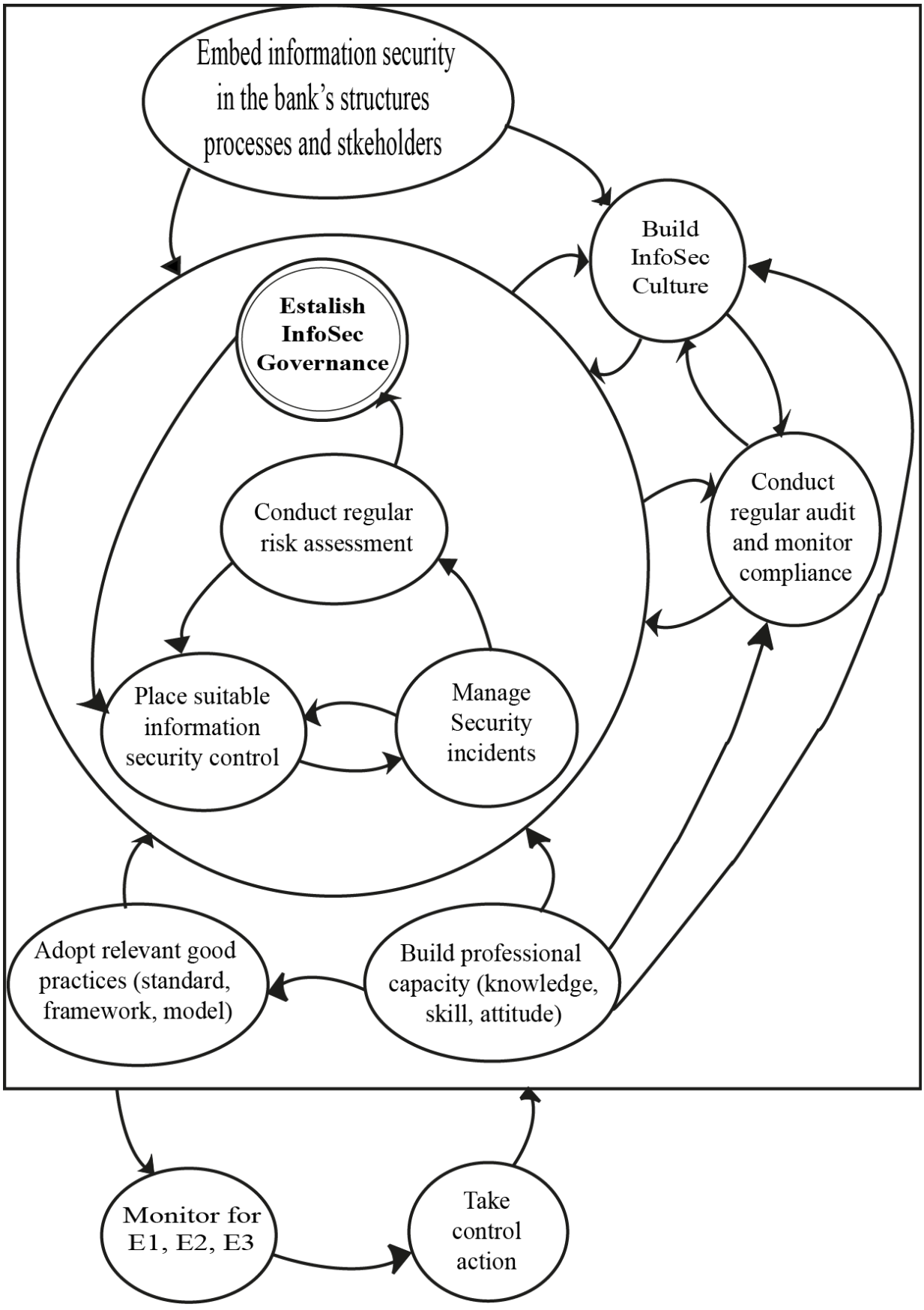

Figure 3: A model of conceptual activities for analysing information security

‘Conduct a regular risk assessments’ is the central activity since the model emphasizes a risk based approach. This activity helps to establish information security governance and place suitable security controls. The activities in the inner subsystem of the model (the circle) influence information security culture and monitoring compliance is achieved through conducting regular audit. Activities in the external subsystem (the rectangle) provides input to the activities in the internal subsystem.

In order to keep the number of activities to a minimum as suggested by Checkland and Poulter (2006), activities in the model are generalised. ‘Establish InfoSec Governance’ is a generalisation of: *develop information security strategy, ensure effective information security leadership, develop policies, procedures and guidelines, create relevant information security processes, prepare information security metrics and measure information security performance*.

The next stage of SSM is to use the conceptual activity model to question the current information security situation against the problematic situation in order to define the required improvement areas or changes. The model helps to prepare questions to ask about the situation.

Questioning the Current Situation Using the Model

The common way to undertake this stage, is to provide a table that consists of activities and connections from the model in one axis and questions to ask about those elements on the other axis (Checkland and Poulter, 2006). The questions that will be addressed are ‘Does each activity exist in the current situation?’ ‘Who does the activity?’ and ‘Is the activity done effectively?’, as presented in Table 2 below.

Table 2: Questioning the current situation using the model

No	Activity		Exists?	Who does it?	Effective?
1	Embed information security in the bank's structures, processes and stakeholders		Partial	Top management and InfoSec Department	No
2	Build InfoSec Culture		Partial	InfoSec Department and National InfoSec Agency	No
3	*Establish InfoSec Governance*	*Develop InfoSec Strategy*	*No*	-	-
4		*Develop policies, procedures & guidelines*	*Partial*	*InfoSec Department and National InfoSec Agency*	*No*
5		*Create InfoSec processes*	*Partial*	*InfoSec Department*	*No*
6		*Strengthen InfoSec leadership*	*Partial*	*Top management*	*Partial*
7		*Prepare InfoSec metrics*	*No*	-	-
8		*Measure performance*	*Partial*	*Top management*	*No*
9	Conduct regular audit and monitor compliance		Partial	InfoSec Department and National InfoSec Agency	Partial
10	Conduct regular risk assessment		Partial	InfoSec and Risk Management Departments	Partial
11	Place suitable information security controls		Partial	All stakeholders	Partial
12	Manage security incidents		Partial	InfoSec Department and National InfoSec Agency	Partial
13	Adopt relevant good practices (standards, framework and model)		Partial	InfoSec Department and E-banking Division	Partial
14	Build professional capacity (knowledge, skill and attitude)		Partial	Top management and InfoSec Agency	Partial
15	Monitor the efficacy (E1), efficiency (E2) and effectiveness (E3) of the ISMS		Partial	InfoSec Department and Top management	Partial
16	Take control actions based on the monitoring outcome		Partial	InfoSec Department and Top management	Partial

Questioning the current situation is followed by defining actions which resolve the problematic situation, and leads to finding arguably desirable and culturally feasible response. (Checkland and Poulter, 2006).

Defining the Action

Any significant change in the real situation usually involves three elements: *making change to structure; changing processes or procedures; and changing attitude* (Checkland and Poulter, 2006). The actions defined based on the activity model will involve one or more of these elements.

A list of actions are required to address the gaps identified. Since none of the activities are complete in Table 2, these comprise the actions. These actions will improve the information security of the bank to ensure the ISMS realises the bank's desired outcomes.

5. Conclusion

The principal aim of this paper was to explore the use of SSM to analyse the socio-technical information security issues in a major bank. A key reason for selecting SSM was that it addresses shortcomings of traditional risk assessment approaches that take a 'hard systems' approach and which focus on system components rather than the system as a whole. It was reasoned that SSM's holistic view is appropriate as banking systems are becoming more complex, attacks are increasing in frequency and *aimed at employees*. SSM is designed for complex and messy situations and has stakeholders (employees) at its heart.

Results clearly showed that SSM is a powerful tool to analyse the bank's ISMS. A critical benefit of the methodology was that it enabled the different attitudes and conceptions of key stakeholders to be modelled in a systemic and systematic way – in stark contrast to traditional risk assessment methodologies.

The bank's current information security situation was expressed using a Rich Picture and a concept map. Not only did these tools prove to be effective for analysis, but they were easily understood by stakeholders which helped validate the analyst's interpretation of the data. Furthermore, James (1996) highlighted benefits of shifting between real-world and ideal world models for action planning. The methodology also enabled a systematic approach to summarising the key issues (questioning the current situation using the

models) and identifying a set of corresponding actions. A further benefit of SSM is that it involves users at all stages, thus member validation is integrated 'automatically' as part of the methodology.

The results show that SSM was effective for analysing messy information security problems which require systems thinking. It was suitable to conduct the analysis, present the discussion, engage with stakeholders and in this way it aligned with effective approaches for assessing culture. Hence it effectively addressed the research questions relating to the status of the ISMS and challenge.

Since the approach is action-oriented it also directly provides potential approaches for improving the problem situation. A further important factor in the success was the selection of key stakeholders from the business, and notably the willingness of senior managers to participate in an open way.

Further validation of the approach was provided by the CISO of the bank through feedback after receiving the report of the study. He emphasized that the process was easy to understand, confirmed the outputs were useful and realistic, and helped them to understand the overall security status of the bank. Subsequently, the bank has started acting on them by initiating an information security strategy development.

It is important to point out that we see SSM complementing current risk assessment approaches, not replacing them. It has uncovered systems issues that traditional approaches do not consider – something that is vital as threats become ever more complex and human-related.

Case study research seeks to an understanding of a complex issue or object and emphasize detailed contextual analysis of a limited number of situations and their relationships. As such, a limitation of this study is lack of generality of results: it cannot be claimed that other banks will have exactly the same security issues. However, this does not mean that results are inapplicable to other situations, on the contrary, they provide a useful checklist that can be used to explore potential security problems. By explaining the approach in detail, this paper bridges theory and practice, and shows how others can adopt SSM in this context.

Future research will extend this work by evaluating the effectiveness of the actions identified, in addressing the socio-technical aspects of information security of the bank.

References

Alfawaz, S.M., 2011. *Information security management: a case study of an information security culture* (Doctoral dissertation, Queensland University of Technology).

Chaula, J.A., 2006. *A socio-technical analysis of information systems security assurance: A case study for effective assurance* (Doctoral dissertation, Stokholm University)

Checkland, P., 1999. Soft Systems Methodology: a thirty year retrospective. In Systems *Research and Behavioral Science*.

Checkland, P.B. & Poulter, J., 2006. *Learning for Action: A short definitive account of Soft Systems Methodology and its use for Practitioners, teachers and Students*, Wiley, Chichester.

Da Veiga, A. & Eloff, J.H., 2007. An information security governance framework. *Information Systems Management*, *24*(4), pp.361-372.

Da Veiga, A. & Eloff, J.H.P., 2010. A Framework and assessment instrument for information security culture. *Computers & Security*. 20 pp. 196-207.

FFA, 2015) *Financial fraud action uk annual review: working together to prevent fraud*, http://www.financialfraudaction.org.uk/, [Accessed on 12/01/2016]

Hagen, J.M, Albrechtsen,E. & Hovden,J., 2008, Implementation and effectiveness of organizational information security measures, *Information Management & Computer Security*, Vol. 16 Iss: 4, pp.377 – 397.

Hamidovic, H., 2011, BMIS—An Introduction to the System Environment. *ISACA JOURNAL*. 4, pp. 1-3.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P., 2011. Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), pp.373-384.

Höne, K., & Eloff, J. H. P., 2002. Information security policy—what do international information security standards say? *Computers & Security*, 21(5), pp. 402-409.

ISACA, 2010. *Business Model for Information Security (BMIS)*. [Online]. Available from: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx. [Accessed on 12/03/2015].

ISACA, 2011. *Creating a Culture of Security*. [Online]. Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx. [Accessed on 18/02/2015].

ISO/IEC, 2013. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements. Switzerland.

James, H.L., 1996, October. Managing information systems security: a soft approach. In *Information Systems Conference of New Zealand, 1996. Proceedings* (pp. 10-20). IEEE.

Karlsson, F., Åström, J. & Karlsson, M., 2015,"Information security culture – state-of-the art review between 2000 and 2013", *Information & Computer Security*, Vol. 23 Iss 3 pp. 246 - 285

Kaspersky Lab, 2015. *The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide*. [Online]. Available from: http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide. [Accessed on 19/03/2015].

Lacey, D. 2009. *Managing the Human Factor in Information Security*, Wiley, London

Lacey, D. 2010. Understanding and transforming organizational security culture, *Information Management & Computer Security*, 18(1), pp. 4 – 13.

Locher, C., 2005. Methodologies for evaluating information security investments-What Basel II can change in the financial industry. *ECIS 2005 Proceedings*, 122.

Mulwa, D.K., 2012. *A survey of insider information security threats management in commercial banks in Kenya* (Doctoral dissertation, University of Nairobi).

Munir, U., & Manarvi, I., 2010. Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks. *Global Journal of Computer Science and Technology*, pp. 10(10).

Ngwenya, B. and Malufu, K., 2012. *Perceptions Towards On-line Banking Security: An Empirical Investigation of a Developing Countrys Banking Sector, how secure is On-line Banking*. International Journal of Computer Science and Network (IJCSN), 1(6), p. 73-81.

OECD, 2015. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf . [Accessed on 19/01/2016].

Okere, I., Van Niekerk, J. & Carroll, M., 2012. Assessing Information Security Culture: A Critical Analysis of Current Approaches. *Information Security for South Africa (ISSA). IEEE*, Johannesburg, 15-17 Aug.

Pinder, P., 2006. Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II). *Information security technical report*, *11*(1), pp.32-38.

Posthumus, S., & Von Solms, R., 2004. A framework for the governance of information security. *Computers & Security*, 23(8), pp. 638-646.

Raytheon/ Websence, 2015. *2015 Industry Drill-down Report: Financial Services*, https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf , [Accessed 23/12/2015]

Reviewer1 (2002?) Assessing Information System Security: An Application for the Soft Systems Methodology

Salvi, V., 2013. *Information Security Management at HDFC Bank: Contribution of Seven Enablers.* [Online]. Available from: http://www.isaca.org/Knowledge-Center/Documents/Information-Security-Management-at-HDFC%20Bank-Contribution-of-Seven-Enablers_1113.pdf. [Accessed on 18/02/2015].

Schein, E., 2009. The Corporate Culture Survival Guide, San Francisco:J ossey-Bass, 2009.

Selamat, M.H. and Babatunde, D.A., 2014. Mediating Effect of Information Security Culture on the Relationship between Information Security Activities and Organizational Performance in the Nigerian Banking Setting. *International Journal of Business and Management*, *9*(7), p.33-38.

Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), pp.31-41.

Susanto, H., Almunawar, M. N., & Tuan, Y. C., 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences IJECS-IJENS.* 11 (5), pp. 23-29.

Symantec, 2012. *Internet security threat report trends for 2011. Volume 17.* https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_17 . [Accessed on 18/12/2015]

Tarimo, C.N., 2006. *ICT security readiness checklist for developing countries: A social-technical approach* (Doctoral dissertation, Stockholm University).

Travelers, 2015. *2015 Travelers Business Risk Index*, https://www.travelers.com/iw-documents/resources/business-risk-index/2015-report.pdf [Accessed 23/12/2015]

Tsiakis, T., Chatzipoulidis, A., Kargidis, T., & Belidis, A., 2011. Information Technology Security Governance Approach Comparison in E-banking. *Security Technology*, pp. 75-84. Springer Berlin Heidelberg.

Udeh, I., & Dhillon, G., 2008. An Analysis of Information Security Governance Structures: the Case of Société Générale Bank. *3rd Annual Symposium on Information Assurance (ASIA'08),* pp. 41-46.

Ula, M., Ismail, Z., & Sidek, Z. M., 2011. A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, pp. 1-12.

Van Niekerk, J.F., Von Solms,R., 2010.Information Security Culture: A Management perspective. *Computers & Security*. 29 pp. 476-486

Von Solms, R., Thomson, K. L., & Maninjwa, M., 2011. Information security governance control through comprehensive policy architectures. *In Information Security South Africa (ISSA)*, (pp. 1-6). IEEE.

Weise, E., 2014. *JP Morgan reveals data breach affected 76 million households. USA TODAY*. [Online]. 3 October. Available from: http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/. [Accessed on 18/02/2015].

Wilson, H, 2013. *Every minute of every day, a bank is under cyber attack,* 06 Oct, [online], Available: http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359563/Every-minute-of-every-day-a-bank-is-under-cyber-attack.html , [Accessed: 03/03/16]

Yin, R. K., 2009. Case Study Research Design and Methods, 4th edition, Applied Social Research Methods Series, Volume 5, SAGE Publications Inc.

Yin, R. K., 2012. Applications of Case Study Research, SAGE Publications Inc.

Zuccato, A., 2007. Holistic security management framework applied in electronic commerce. *Computers & security*, *26*(3), pp.256-265.

[i] Personal Communication.

[ii] The pictures on the Figure are taken from different websites.